Data Protection Policy

Contents

1. Introduction

Whitehouse Village Hall (WVH) processes the personal data of living individuals such as its trustees, Committee, volunteers, staff, contractors, suppliers (where they are individuals) and customers. This processing is regulated by UK Data Protection Legislation. The Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR) provide the comprehensive framework for data protection in the UK, alongside the Privacy and Electronic Communications Regulations 2003 (PECR). The Information Commissioner (ICO) is the UK's Supervisory Authority for data protection.

As a data controller WVH must comply with the data protection principles with respect to personal data. This policy describes how WVH will ensure continuing compliance with the DPA in general, the data protection principles and rights of individuals in particular.

2. Reference documents

- UK GDPR (the retained version of Regulation (EU) 2016/679 as amended for UK law)
- Data Protection Act 2018 (DPA)
- UK Data (Use and Access) Act 2025
- Privacy Policy
- Data Breach Response & Notification Procedure
- Data Breach Response PR & Communications Guidance
- Subject Access Request Policy
- Data Subject Rights Policy

3. Purpose

This policy forms part of WVH's commitment to the safeguarding of personal data processed by its staff. Processing has a very broad definition, and includes activities such as using, storing, amending, analysing, disclosing and destroying data. The policy will:

- help staff recognise personal data
- help them understand their rights
- help them understand their obligations to WVH, in respect of all WVH personal data and special categories of data

4. Scope

This policy applies to all those individuals and organisations that process personal data on behalf of WVH, including but not limited to:

- Employees, consultants, contractors and temporary workers
- Trustees, committee members and all other voluntary workers for WVH
- Individuals who work for clients and suppliers and who are WVH contacts
- Arms' length organisations associated with, and officially recognised by WVH
- Third parties associated with WVH.

5. Definitions

Personal Data
Personal data means any information relating to an identified or identifiable living person who can be identified directly or indirectly from a name, identification number, location data, an online identifier (e.g. IP address) or one or more specific factors such as the physical, physiological, genetic, mental, economic, cultural or social identity of that living person.

Data Subject
An identified or identifiable living individual who is the subject of personal data.

Anonymisation
Data are anonymised if they no longer relate to an identified or identifiable individual. The principles and rules of data protection do not apply to anonymised information.

Pseudonymisation
This process is a measure by which personal data cannot be attributed to the data subject without additional information, which is kept separately. The 'key' that enables re-identification of the data subjects must be kept separate and secure. Data that have undergone a pseudonymisation process remain personal data. There is no concept of 'pseudonymised data' under UK law.

The principles and rules of data protection apply to pseudonymised data.

Special categories of personal data (previously referred to as 'sensitive data') is:

- the racial or ethnic origin of individuals
- their political opinions
- their religious beliefs or philosophical beliefs
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)
- data concerning health
- data concerning a person's sex life or sexual orientation
- genetic data
- biometric data for the purpose of uniquely identifying a living person

The UK GDPR defines data concerning 'health', as personal data related to the physical and mental health of a person, including the provision of health care services which reveal information about his or her health status. The term broadly includes medical diagnosis, assessment of an employee's capacity for work, DNA sequences, medical research, treatment and the management of healthcare services.

Personal data relating to criminal convictions etc. is not included in the definition. But processing of this data outside of the control of official authority must be authorised by domestic law, which provides for safeguards.

Personal data, such as personal addresses and financial data (including salaries) are not sensitive personal data but should be treated with similar care.

Manual Personal Data
Personal data recorded as part of a structured filing system or intended to be contained in a filing system in paper form, or another non-electronic format.

Processing
Obtaining, recording or holding personal data. This includes organisation, adaptation or alteration; retrieval, consultation or use; disclosure; and alignment, combination, blocking, erasure or destruction.

Filing System
Means any structured set if personal data which can be readily accessed according to specific criteria on a functional or geographical basis. Files can be held by automated means or manually. If files are not structured, they are not covered by the DPA.

Data Holding
A collection of one or more data sets or files that are being processed for permitted purposes under the direction of a clearly identified member of WVH staff - the Data Owner.

Data Controller
The organisation which determines the means and purposes of the processing, WVH is the Data Controller for the personal data that it processes.

Joint controllers
a) Where two or more data controllers jointly determine the purposes and means of processing personal data for a shared purpose, they are joint controllers;
b) Joint controllers must, in a transparent manner, determine their respective responsibilities for compliance with data protection by means of a contractual arrangement between them. (There is an exception to the extent that those responsibilities are determined under or by virtue of an enactment).
c) The arrangement must designate the controller which is to be the contact point for data subjects.

Data Protection Representative
The registered representative based in one of the Member States where processing takes place and contracted to act on behalf of WVH in the EEA. In particular, the role is to communicate with the supervisory authorities and data subjects in accordance with Article 27 of the UK GDPR.

Privacy Officer/Data Protection Officer
The WVH member of staff with lead responsibility for WVH's compliance with the applicable data protection legislation.
OR
The formally appointed external Data Protection Officer Service provided by Data Compliant Limited to fulfil the mandatory DPO duties. Such duties are detailed in Article 39 of the UK GDPR.

Data Owner
The WVH member of staff with lead responsibility for permitting and managing the retention and processing of a data holding for which WVH is the Data Controller. Data Owners delegate responsibility for personal data elements to Data Custodians.

Data Custodian
The individual unit or person identified by the data owner to be responsible for the collection, creation, modification and deletion of specified personal data element(s)

System Custodian

A person appointed by a Head of Department with responsibility and authority to implement the Information Security Policy and supporting policies in respect of an WVH-wide or departmental system, to ensure that the security measures adopted for systems under his/her control meet the requirements of these policies and to carry out the duties as set out in the associated Codes of Practice. In the case of a large system some duties may be delegated, to named persons whose particular duties are set out in writing, although the Custodian retains overall responsibility for the security of that system.

Data Processor
Any third party who processes personal data on behalf of and on the written instructions of the Data Controller. The written instructions must be a data processing agreement or similar formal contractual agreement with the relevant data protection clauses.

Profiling
Means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Recipient
In relation to personal data, means any person to whom the data is disclosed, whether a third party or not, but it does not include a public authority to whom disclosure is or may be made in the framework of a particular inquiry in accordance with the law.

Public Authority and Public Body
The terms 'public authority' or 'public body' are not defined in the UK GDPR. The DPA 2018 adopts Freedom of Information Act 2000 and Freedom of Information (Scotland) Act 2002 definitions see extract below:

'*(1)For the purposes of the UK GDPR, the following (and only the following) are "public authorities" and "public bodies" under the law of the United Kingdom— (a) a public authority as defined by the Freedom of Information Act 2000, (b) a Scottish public authority as defined by the Freedom of Information (Scotland) Act 2002 (asp 13), and (c) an authority or body specified or described by the Secretary of State in regulations, subject to subsections (2), (3) and (4).*

(2) An authority or body that falls within subsection (1) is only a "public authority" or "public body" for the purposes of the UK GDPR when performing a task carried out in the public interest or in the exercise of official authority vested in it.

(3) The references in subsection (1)(a) and (b) to public authorities and Scottish public authorities as defined by the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002 (asp 13) do not include any of the following that fall within those definitions— (a) a parish council in England; (b) a community council in Wales; (c) a community council in Scotland; (d) a parish meeting constituted under section 13 of the Local Government Act 1972; (e) a community meeting constituted under section 27 of that Act; (f) charter trustees constituted— (i) under section 246 of that Act, (ii) under Part 1 of the Local Government and Public Involvement in Health Act 2007, or (iii) by the Charter Trustees Regulations 1996 (S.I. 1996/263).
(4) The Secretary of State may by regulations provide that a person specified or described in the regulations that is a public authority described in subsection (1)(a) or (b) is not a "public authority" or "public body" for the purposes of the UK GDPR'.

Personal data breach
Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

6. Policy Statement

Lawful processing of personal data is vital to the successful operation and reputation of WVH, and for maintaining the trust of our employees, customers and other stakeholders. WVH is committed to protecting the rights and freedoms of individuals in accordance with the provisions of data protection legislation. In order to achieve this, WVH shall ensure that personal data is handled appropriately and consistently in line with the UK GDPR and DPA 2018.

WVH shall ensure that personal data is:

- Processed lawfully, fairly and in a transparent manner in relation to individuals
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data shall be stored for longer periods insofar as the personal data shall be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of individuals
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

WVH, as a data controller, shall be responsible for, and be able to demonstrate, compliance with the principles of data protection legislation (see 6.1.2 below).

All processing of personal data by third parties on behalf of WVH, where WVH is data controller, shall be covered by contract and include adequate data protection clauses.

6.1 The Data Protection Principles

These are specified in Article 5 UK GDPR, see the summary below:

1. Processing of personal data must be lawful, fair and transparent in relation to the data subject.

    a) **Lawful** processing requires either: consent of the data subject, necessity to enter a contract; necessity to protect the vital interests of the data subject or of another person; necessity for performing a task in the public interest; necessity for the legitimate interests of the controller or a third party, if they are not overridden by the interests and rights of the data subject
    b) **Fair** processing means the data subject must be informed of the risk to ensure that processing does not have unforeseeable negative effects.

c) **Transparent** - Personal data processing should be done in a transparent manner. Controllers must inform data subjects before processing their data, among other details, about the purpose of processing and about the identity and address of the controller. Information on processing operations must be provided in clear and plain language to allow data subjects to easily understand the rules, risks, safeguards and rights involved. Data subjects have the right to access their data wherever they are processed.

d) In the case of special categories of data at least one of the conditions in Article 9 or Article 10 must also be also met. Article 9 Conditions include the following:

- The data subject has given explicit consent to the processing for a specified purpose
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law providing for appropriate safeguards for the fundamental rights and interests of the data subject
- Processing is necessary to protect the vital interests of the data subject or another living person where the data subject is physically or legally incapable of giving consent
- Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim
- Processing relates to personal data which are manifestly made public by the data subject
- Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
- processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to conditions and safeguards
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Processing personal data relating to criminal convictions and offences must be processed in accordance with Article 10 which states that processing of this category of data outside of the control of official authority must be authorised by domestic law, which provides for safeguards.

Processing special categories of data under the DPA must in addition to Article 9, and 10 above comply with the Schedule 1 grounds for processing and if so have a supporting policy document

for procedures for compliance with the Principles and Policies for retention and erasure of such data.

2. The purpose must be defined before processing is started. The principle of **purpose limitation** means that any processing of personal data must be for a specific, well defined purpose and only for additional, specified, purposes that are compatible with the original purpose or purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed (**data minimisation**).

4. Personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to erase or rectify inaccuracies without delay. Data may need to be checked regularly and kept up to date to secure **accuracy**.

5. Personal data processed for any purpose or purposes must not be kept for longer than is necessary for that purpose or those purposes to be completed. Personal data kept in an identifiable form should be deleted or anonymised (**storage limitation**). Personal data may be stored for longer periods in so far as personal data will be solely processed for archiving purposes in the public interest, scientific or historical research or statistical purposes in accordance with Article 89 (1) subject to appropriate technical and organisational measures. Time limits should be set for erasure or periodic review of continued storage.

6. Personal data must be processed in a way that ensures that appropriate technical and organisational measures be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (**integrity and confidentiality**). The data controller should take into account the "state of the art, the costs of implementation and the nature scope, context and purpose of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons". Depending on the specific circumstances of each case, appropriate technical and organisational measures could include, for example, pseudonymising and encrypting personal data and/or regularly testing and evaluating the effectiveness of the measures to ensure the data processing is secure

Accountability – As a data controller WVH is responsible for and must be able to actively and continuously demonstrate compliance with the principles for all data processing activity.

Controllers must be able to demonstrate compliance with data protection provisions to data subjects, the general public and supervisory authorities at any time

Controllers can facilitate compliance with this requirement in various ways, which include:

- recording processing activities and making them available to the supervisory authority upon request;
- in certain situations, designating a data protection officer who is involved in all issues relating to personal data protection;
- undertaking data protection impact assessments for types of processing likely to result in a high risk to the rights and freedoms of individuals;
- ensuring data protection by design and by default;
- implementing modalities and procedures for the exercise of the rights of the data subjects;
- adhering to approved codes of conduct or certification mechanisms

6.2 Rights of the data subject

In addition to the principles WVH must uphold with the **rights of individuals** which are as follows:

a) **Right to information** at the point at which personal data is collected (as stated in the WVH Privacy Policy and privacy statements)

b) **Right of access** – individuals have the right to request access to the information held by WVH. Such processing is documented in the WVH Subject Access Request Policy.

c) **Right to data portability** – allows individuals to obtain and reuse their personal data for their own purposes across different services where processing is based on consent or performance of a contract. It allows them to; move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The personal data must be provided in a structured, commonly used and machine-readable form. The information must be provided free of charge

d) **Right to object to processing** (including for the purposes of direct marketing and which includes profiling to the extent that it is related to direct marketing). They can also object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority, and processing for purposes of scientific/historical research and statistics.

e) **Right not to be the subject of automated decision making**, including profiling. The controller may not take a decision significantly affecting a data subject that is based solely on automated processing of personal data relating to the data subject.

f) **Right to rectification** (have incomplete or inaccurate personal information corrected). This must be done without undue delay. Where appropriate a supplementary statement can be provided e.g. where the rectification relates to a matter of fact.

g) **Right to erasure** (right to be forgotten, in specific circumstances). Those circumstances are but not limited to: where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; when the individual withdraws consent; when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing; when the personal data was unlawfully processed; when the personal data has to be erased in order to comply with a legal obligation.

h) **Right to lodge complaint** Data subjects are entitled to submit complaints first to WVH under our internal complaints process, as required by the DUAA. If unresolved, individuals may escalate complaints to the Supervisory Authority (ICO)

i) Right to compensation

6.3 Transfers outside the UK

Personal data must not be transferred to a country or territory outside the UK unless that country or territory ensures an adequate level of protection for the rights and freedoms of data

subjects in relation to the processing of personal data, as determined by the UK government. The UK has adopted adequacy regulations for certain countries and territories. Transfers to third countries can be governed by the UK International Data Transfer Agreement (IDTA), UK Addendum to the EU Standard Contractual Clauses (SCCs), or Binding Corporate Rules. The EU-US Privacy Shield is no longer valid for UK-US transfers.

7. Sharing of Personal Data

Ensuring that personal data is shared appropriately is vital to the successful operation and the reputation of WVH, and for maintaining the trust of our employees, customers and other stakeholders. In order to achieve this, WVH shall:

- Undertake a data protection impact assessment screening for any new initiatives that involve the sharing of personal data. Where sharing is likely to result in a high risk to the rights and freedoms of natural persons (particularly where new technology is involved) a full data protection impact assessment shall be completed.
- Identify a clear objective, or set of objectives, for the sharing of personal data
- Identify a lawful basis in data protection legislation for the sharing of personal data
- Ensure that the sharing of personal data is necessary to achieve the identified objective(s). Anonymised or pseudonymised data shall be shared where the identification of data subjects is not required
- Share the minimum amount of personal data required to achieve the objective(s)
- Provide data subjects with privacy notices and, where data subjects have a choice, seek consent for the sharing of their personal data
- Clearly distinguish factual information from opinions
- Record all decisions to share personal data
- Ensure that a written agreement between the parties to a data sharing arrangement is in place where personal data is shared on a systematic basis or there is a large-scale transfer of personal data. Such agreements shall, as a minimum, include:

    - The classes, or specific items, of personal data to be shared
    - The source(s) of the personal data
    - The objective(s) of the data sharing arrangement
    - The lawful basis for sharing the personal data
    - The individuals/groups that will have access to the personal data
    - The methods by which the personal data will be transferred, including any controls for protecting the data from loss, destruction or unauthorised access
    - The frequency with which the personal data will be shared
    - Storage requirements for the personal data, including any controls for protecting the data from loss, destruction or unauthorised access
    - The parties' responsibilities for ensuring the accuracy of the personal data
    - Retention and disposal requirements
    - Arrangements for enabling data subjects to exercise their rights
    - Processes and procedures for handling information security incidents.

8. Appointment and Support of the Data Protection Officer (DPO)

WVH has formally assessed and documented the need for a Data Protection Officer on an annual basis. At this stage of the Companies development a DPO as referenced in Article 39 of the UK GDPR is not deemed necessary.

9. Roles and Responsibilities

9.1 Executive Committee shall ensure that the purposes and means of processing of personal data for which WVH is data controller are determined in compliance with legislation.
Responsibility for ensuring implementation of, and compliance with, this policy will be in accordance with WVH's line management structure.

9.2 All individuals and organisations that process personal data on behalf of WVH shall comply with this policy and associated data protection, information security, information management and information technology regulations, policies, processes and procedures.

9.3 The Data Protection Officer (DPO) is an advisory role and is concerned with WVH's compliance with data protection legislation. The DPO shall:

- provide advice, assistance and recommendations to the [Information Risk Owner (IRO)] in relation to data protection risks
- enable compliance with data protection legislation
- play a key role in fostering a data protection culture within WVH
- help implement essential elements of data protection legislation, such as the principles of data processing, data subjects' rights, data protection by design and by default, records of processing activities, security of processing and notification and communication of data breaches
- review the planning, implementation and progress of WVH's data protection initiatives periodically, reporting to the [Board]
- advise the IRO in relation to any breaches of data protection legislation
- be WVH's point of contact with the Supervisory Authority.
- The DPO shall not determine the purposes of processing personal data, or the means by which any personal data processing activity is done.

9.4 The Information Risk Owner (IRO) is an accountable role and is concerned with the management of all information assets held by WVH. With regards personal data, the IRO shall have overall responsibility for:

- the processing of personal data (of which WVH is data controller) in compliance with data protection legislation, including the appropriate determination of the purposes of processing personal data, and the means by which any personal data processing activity is done
- ensuring that the DPO is involved properly, and in a timely manner, in all issues which relate to the protection of personal data, that the opinion of the DPO is given due weight and that the DPO is consulted promptly once a data breach or another incident has occurred.
- the management of data protection risks
- planning, implementing and progressing WVH's data protection initiatives
- managing the implementation of essential elements of data protection legislation, such as the principles of data processing, data subjects' rights, data protection by design and by default,

records of processing activities, security of processing and notification and communication of data breaches
- managing the response to breaches of data protection legislation
- ensuring that an effective monitoring and reporting framework is established with regards data protection compliance, and that information asset owners and super information asset owners are designated, perform their roles and report regularly on data protection compliance in relation to their respective information assets and business units
- ensuring that no individual is given access to personal data without having undertaken appropriate training and read relevant policy and guidance.
- The IRO shall also play a key role in fostering a data protection culture within WVH.

9.5 Information Asset Owners shall:

- ensure that personal data held within their respective business units are processed in compliance with this policy
- identify and manage data protection risks within their respective business units
- no individual is given access to that personal data without having undertaken appropriate training and read relevant policy and guidance
- ensure that local processes and procedures are developed, implemented, followed and regularly reviewed
- monitor and report on compliance in their business units as required by WVH.

9.6 Third parties processing personal data on behalf of WVH shall comply with this policy alongside any specific terms and conditions agreed contractually.

An investigation will be undertaken by the Data Breach Response team leader immediately and wherever possible, within 24 hours of the breach being discovered / reported.

The Data Breach Response team leader will investigate the breach and assess the risks associated with it, for example, the potential adverse consequences for individuals, how serious or substantial those are and how likely they are to occur.

The investigation will need to take into account the following:

- the type of data involved;
- its sensitivity;
- the protections are in place (e.g. encryptions);
- what has happened to the data (e.g. has it been lost or stolen);
- whether the data could be put to any illegal or inappropriate use;
- data subject(s) affected by the breach, number of individuals involved and the potential effects on those data subject(s);
- whether there are wider consequences to the breach.

10. Security of Personal Data

All staff processing personal data should ensure that the data are secure: appropriate measures must be taken to prevent unauthorised access, disclosure and loss. Staff whose work includes responsibility for supervision of contractors and third parties have a duty to ensure that they observe the principles of the UK GDPR.

It is rarely necessary to store electronic personal data on portable devices such as laptops, USB flash drives, portable hard drives, or any computer not owned by WVH. Similarly, hard copy personal data should not be regularly removed from WVH premises. In the case of electronic data, to minimise the risk of loss or disclosure, a secure remote connection to WVH should always be used.

Downloading personal data on to portable devices or taking manual personal data off-site must be authorised in writing by the Data Owner, who must explain and justify the operational need in relation to the volume and sensitivity of the data. The data must be strongly encrypted. Users should only store the data necessary for their immediate needs and should remove the data as soon as possible. To avoid loss of encrypted data, or in case of failure of the encryption software, an unencrypted copy of the data must be held in a secure environment. The [Information Security] Team's guidance on encryption should be followed.

Hard copy personal data and portable electronic devices should be stored in locked units, and they should not be left on desks overnight or in view of third parties.

In order to comply with the fifth data protection principle personal data should be securely destroyed when no longer needed, with consideration for the format of the data. The [Information Security] Team's guidance should be followed for electronic data.

Personal data must not be disclosed unlawfully to any third party. Transfers of personal data to third parties must be authorised in writing by the data owner and protected by adequate contractual provisions or data processor agreements, agree with WVH's notification and must use safe transport mechanisms.

All losses of personal data must be reported immediately to the WVH Privacy Officer in accordance with the WVH Breach Response Policy. Negligent loss or unauthorised disclosure of personal data, or failure to report such events, may be treated as a disciplinary matter and could be considered gross misconduct.

11. Access to Personal Data

11.1 Subject access rights

A subject access request must be handled in accordance with the WVH Subject Access Request Policy. Data subjects have a right of access to their personal data, including some unstructured manual personal data. Subject access requests must be made in writing, including Form [Control Document] or otherwise and sent to the [Data Privacy Officer]. Data subjects must prove their identity.

Copies will be provided in permanent form promptly and in any event within 30 days.

Some personal data are exempt from the right of subject access, including confidential references provided by WVH.

When responding to a Subject Access Request, WVH will conduct **a reasonable and proportionate search** of relevant records, as clarified by the DUAA.

WVH does not charge a fee for subject access requests.

11.2 Monitoring

It is sometimes necessary for WVH to monitor information and communications. This may include personal data.

11.3 Third party access

In certain circumstances the DPA / UK GDPR provides for disclosure of personal data, without the consent of the data subject, to certain organisations. Requests for such disclosures from third parties, such as the police, UK Border Agency, local authorities or sponsors, should be made in writing and handled by the Data Privacy Officer. This will ensure the validity of the request and any warrants or orders of court can be checked. Staff disclosing personal data may not be protected by an invalid warrant.

12. Records management

Records in all formats containing personal data must be created, stored and disposed of in accordance with WVH's procedures and codes of practice. They must be authentic, reliable and usable and capable of speedy and efficient retrieval.

They must be kept for no longer than the periods permitted in WVH's retention schedule [Record Retention Policy] and, when no longer needed for operational reasons, must be transferred to WVH's in-house records storage facility or archive (if selected for permanent preservation) or disposed of securely and confidentially.

13. Breaches of Policy

All breaches of this policy and data protection legislation shall be reported immediately in accordance with WVH's Information Security Incident Reporting Procedure.

Third parties shall report via their WVH point of contact. Breaches shall be managed in accordance with WVH Information Security Incident Management Procedure.

A breach of this policy by an employee may result in disciplinary action. A breach by a third party may result in a termination of contract and/or compensation claim.

14. Policy Review and Maintenance

This policy will be updated as necessary to reflect best practice and to ensure compliance with any changes or amendments to relevant UK legislation.

This policy shall be reviewed by WVH's [IRO] and [DPO] annually or whenever there is a significant change in legislation, strategy or organisation. Major changes shall be approved by the WVH Board.

Version	Purpose/change	Author	Date
1.0	Initial release	ASCS	30/10/2020
1.1	Annual review	ASCS	27/12/2025

Whitehouse Village Hall Management Committee

Adopted November 2020 *(next review date January 2027)*